Note to the Reader: Throughout this index boldfaced page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

**A**
- A (Host) records, 140
- AAA records, 140
- AAAs of security, 96, 196
- Accept All Cookies option, 260
- access control in physical security, 196–198, 196
- Access Control Lists (ACLs), 148
- Access Services role, 138
- accidental damage, 63
- Account Is Locked Out option, 53
- Account Lockout Duration setting, 52–53
- Account Lockout Policy setting, 51–53, 52, 206
- Account Lockout Threshold setting, 52
- Account Logon policy, 99
- Account Management auditing, 98, 103
- Account Policies settings, 205, 205
- accounting in AAAs of security, 96, 96
- accounts
  - administrator. *See* administrator accounts
  - auditing, 103
  - lockout policies, 51–53, 52, 206
  - logon events, 101
  - logon policies, 99
  - unlocking, 53–54, 53–54
- acknowledges (ACK) flag, 149
- ACLs (Access Control Lists), 148
- Active Directory
  - combining services with, 137
  - permissions, 87–91, 88–90
- Active Directory Domain Services (AD DS)
  - auditing, 102
  - combining services with, 137
  - enabling, 109–110
  - enterprise CAs, 254
- Active Directory-Integrated (ADI) zones, 143
- Active Directory Users and Computers (ADUC) tool
  - account lockout, 54
  - auditing, 108
  - passwords, 55
  - permissions, 87–89, 88
- ActiveX controls, 270–271
- AD CS (Active Directory Certificate Services)
  - CAs, 243, 254
  - combining services with, 137
- AD DS (Active Directory Domain Services)
  - auditing, 102
  - combining services with, 137
  - enabling, 109–110
  - enterprise CAs, 254
- adapters, wireless, 172
- add-ons for IE, 266–268, 267
- address bar in IE, 258
- addresses
  - IP
    - IPv6, 140
    - NAT, 159
    - wireless routers, 183
  - MAC, 187–188, 188
- ADI (Active Directory-Integrated) zones, 143
- Adleman, Leonard, 222
- administrative vulnerabilities, MBSA for, 115
administrator accounts
dual accounts, 62–63
for malware, 28–29
password security for, 194
principle of least privilege, 9–10
tokens, 122
ADUC (Active Directory Users and Computers)
account lockout, 54
auditing, 108
passwords, 55
permissions, 87–89, 88
Advanced Encryption Standard (AES)
encryption, 217
BitLocker, 235
decrypting, 219
overview, 177, 218–219
Advanced Security Settings dialog box, 109, 109
Advanced tab for IE, 268–269, 268
AH (Authentication Header) in IPsec, 165
AIC triad, 1, 4–5, 4
availability, 5–6
confidentiality, 5
integrity, 6–7
alarms, 198
alert levels in Microsoft Security Essentials, 32
algorithms, encryption, 175
All Removable Storage Classes category, 210
All Removable Storage Classes: Deny All Access
setting, 211, 211
Allow Log On Locally option, 206–207, 207
Allowed RODC Password Replication group, 140
Always Notify Me When setting, 124
Annual Security Report, 27
Anti-Phishing Working Group (APWG), 38
antivirus (AV) software and techniques, 28
email, 39–40
installing, 16
mobile devices, 212
working with, 29–31, 29–30
“Apple Smashes Patch Record with Gigantic Update”, 15
appliances, 154
application-layer filtering firewalls, 154
application server services, 137
application testing for buffer-overflow attacks, 26
AppLocker program, 134
Apply Security Policy page, 13
APWG (Anti-Phishing Working Group), 38
Archive The Log When Full, Do Not Overwrite
Events option, 112
archived files, auditing, 114
asymmetric encryption
AES, 177
e-mail, 228
overview, 219–222, 221
attachments in e-mail, 21
attack surfaces
malware, 28
reducing, 11–14, 11–14
attackers, 7
attacks. See malware
attrib command, 73
auditing and audit policies, 95
Account Management, 103
in defense-in-depth strategy, 8
Directory Service Access, 102–103
exercises, 118
logon, 101–102
networks, 114–117, 115, 117
object access, 99–100, 100–101
overview, 96–99, 96–97
Policy Change, 105
Privilege Use, 104–105, 104
review questions, 118–119
security logs, 111–114, 112–113
summary, 117–118
system events, 103
viewing audit information, 110–111, 110–111
Auditing Entry dialog box, 109, 109
Auditing tab, 100, 100
auditpol command, 102
authenticated denial of existence, 168
authentication, 8, 43
  in AAAs of security, 96, 96
  biometrics, 60–61
  certificates for, 242–243
DNS, 167–168
dual administrator accounts, 62–63
exercise, 67
factors, 44
vs. identification, 44–45
Kerberos, 63–64
passwords for. See passwords
RADIUS, 64–65
review questions, 67–68
smart cards and token devices, 59–60, 59–60
starting applications with Run As Administrator, 61–62, 62
summary, 67
unsecure authentication protocols, 65–66
Authentication Header (AH) in IPsec, 165
authentication servers in WPA2, 178
authenticators in WPA2, 178
authorization in AAAs of security, 96, 96
Automatic Updates, 15, 126–128, 127
AV (antivirus) software and techniques, 28
  email, 39–40
  installing, 16
  mobile devices, 212
  working with, 29–31, 29–30
availability, 2, 5–6

B
back-to-back network configuration, 157
backups
  for availability, 5–6
  Security logs, 114
badges, 197
base frequency in wireless security, 172
Basic User software rule, 134
biometrics, 60–61
BitLocker Drive Encryption, 235, 235
  AES for, 218
  BitLocker To Go, 218, 237–238, 238
  recovery keys, 236
  requirements, 235–236
Blaster worm, 23
Block All Cookies option, 260
block ciphers, 176
Blowfish algorithm, 218
bluejacking attacks, 212
Bluesnarfing, 212
Bluetooth devices, 212
botnets
  in DDoS attacks, 149
  and malware, 20–21
  spam from, 27, 141
boundary control for buildings, 196, 196
broadcasts by wireless routers, 185–187
browser history, deleting, 265, 266
brute-force password attacks, 46
buffer overflows
  description, 20
  overview, 25–26, 25
  updates for, 23
buildings, securing, 196–197, 196

C
cable for wireless routers, 174
cache poisoning, 39
cameras, 196
cancel option for inherited permissions, 78
capturing traffic data. See sniffers
CAs. See certification authorities (CAs)
CD And DVD setting, 209
.cer extension, 242
certificate chains, 250, 252–254, 252–253
certificate revocation lists (CRLs), 245–246, 246
Certificate software rule, 135
certificates, 241–242, 241
   ActiveX controls, 270–271
errors, 245–248, 246–248
health, 162
keys, 242–245, 244
PKI, 251
properties, 248–250, 249–251
purposes, 242–243
services, 254–255
certification authorities (CAs)
certificate chains, 253, 253
certificate revocation lists from, 245–246
description, 241, 243
HRA, 164
PKI, 251
Certification Path tab, 250, 251
Certified Information Systems Security
Professional (CISSP) certification, 3
Challenge Handshake Authentication Protocol (CHAP), 65
Change permission, 83
Change Permissions permission, 73
Change User Account Control Settings option, 123
changing passwords, 57–58
CHAP (Challenge Handshake Authentication Protocol), 65
Check For Updates But Let Me Choose Whether To Download And Install Them option, 128
CIA triad, 1, 4–5, 4
availability, 5–6
confidentiality, 5
integrity, 6–7
cipher locks, 197–198
CISSP (Certified Information Systems Security Professional) certification, 3
Clear Log option, 113
Client (Respond Only) policy, 165–166
clients
   in defense-in-depth strategy, 8
   exercises, 144
   Group Policy, 129–130, 130
health evaluation, 162–163, 162
offline folders, 130–133, 132–133
review questions, 144–145
software-restriction policies, 133–135, 134
summary, 144
UAC, 122–125, 122–124
   updating, 125–130, 127, 129–130
clusters, failover, 6
Co-owner permission, 83
code-signing certificates, 243, 270–271
collisions, switches for, 199, 200
combining permissions, 75–76, 76, 85–87
command-and-control servers, 21
commonly used ports, 152–153
compact privacy policies, 261, 261
computer accounts, auditing, 103
Computer Configuration node, 204
collectors
   GPOs for, 203–204
   physical security, 194
Conficker worm, 22
confidentiality, 2
   encryption for. See encryption
   protecting, 5
Connect Even If The Network Is Not Broadcasting option, 186
Connection tab for wireless settings, 182, 182
content-filtering firewalls, 154
Continue To This Website (Not Recommended) option, 248
Contributor permission, 83
cookies, 260–262, 261
copied files, permissions with, 78–81, 80, 233–234
core security principles, 1
defense-in-depth strategy, 7–9, 8
   exercises, 17
   hardening servers, 10–16, 11–14
   principle of least privilege, 9–10, 10
   review questions, 17–18
   risk overview, 1–4, 2
   security triad, 4–7, 4
   summary, 16–17
   cracking passwords, 46–47, 66
Create A Password Reset Disk page, 59
Create All Child Objects permission, 89
Create Files/Write Data permission, 74
Create Folders/Append Data permission, 74
CRLs (certificate revocation lists), 245–246, 246
Cumulative permissions, 88
Custom Classes setting, 209

D
damage
   accidental, 63
   physical, 195
Data Encryption Standard (DES), 217–218
data in defense-in-depth strategy, 8
data integrity, 2
   DNS records, 168
   email, 228–229
   protecting, 6–7
DDoS (distributed denial of service) attacks, 149
decryption, 175, 216–217, 217, 219
Default Domain Policy, 49, 49, 201
Default Domain Controllers Policy, 201, 207, 209
Default - Notify Me Only When Programs Try To
   Make Changes To My Computer option, 124
defaults
   GPOs, 200–201
   IE security level, 269
   wireless router passwords, 183, 185
defense-in-depth strategy
   firewalls in, 155
   methods, 7–9, 8
Define These Policy Settings option, 106, 208
definitions, anti-virus, 31
Delegation of Control Wizard, 90, 90
Delete permission, 74
Delete all Child Objects permission, 90–91
Delete Subfolders and Files permission, 74
deleting browser history, 265, 266
demilitarized zones (DMZs), 158
denial of service (DoS) attacks, 148–149, 148
Denied RODC Password Replication group, 140
Deny Log On Locally option, 207–208, 209
designated recovery agent (DRA), 233
Desktop
   dimmed, 123
   Microsoft Security Essentials on, 31–33, 32
   Details tab for certificates, 250, 250
DHCP (Dynamic Host Configuration Protocol)
   DNS services combined with, 138
   dynamic DNS updates, 142, 142
   enforcement, 163
   wireless routers, 174
dictionary password attacks, 46
Diffie, Whitfield, 222
Diffie Hellman algorithm, 222
digital signatures, 225, 228–231, 229–230, 243
digitally signed email, 228–231, 229–230
dimmed Desktop, 123
dimmed settings, 77
Directory Service Access policy
   auditing, 102–103, 108–110, 109
   description, 99
   automatic display of pictures, 40
   DSA events, 103
   log on locally, 206–208, 207, 209
   SSID broadcasts, 186–187, 187
   Disallowed software rule, 133
   display of pictures, disabling, 40
distributed denial of service (DDoS) attacks, 149
divide-by-zero errors, 26
DMZs (demilitarized zones), 158
DNS. See Domain Name System (DNS) service
DNS Server service properties page, 10, 10
DNSsec (DNS Security Extensions), 167–168
Do Not Overwrite Events (Clear logs Manually)
   option, 112
domain controllers
   DNS on, 143
   RODCs, 139–140, 195
Domain Name System (DNS) service, 140
   authentication, 167–168
   cache poisoning attacks, 39
   DHCP services combined with, 138
dynamic updates, 141–143, 142–143
e/mail spoofing, 141
in pharming, 39
records, 140–141
domains, creating OUs in, 202–203
DoS (denial of service) attacks, 148–149, 148
Downadup worm, 22
Download Them But Let Me Choose Whether To Install Them option, 128
downloads
drive-by, 272
unsafe, 273
viruses in, 22
Downup worm, 22
DRA (designated recovery agent), 233
drive-by attacks, 16
drive-by downloads, 272
dual administrator accounts, 62–63
dynamic DNS updates, 141–143, 142–143
Dynamic Host Configuration Protocol (DHCP)
  DNS services combined with, 138
dynamic DNS updates, 142, 142
  enforcement, 163
  wireless routers, 174

E
EAP (Extensible Authentication Protocol), 64, 178–179
eavesdropping attacks, 149
education for malware, 28
EFS (Encrypting File System), 132, 231–234
  802.1x standards
    enforcement, 163
    overview, 171–172
    Windows 7 wireless settings, 181
elevated administrator tokens, 62
email, 225
  antivirus software for, 29
  attachments, 21
digitally signed, 228–231, 229–230
encrypting, 226–228, 226–228
  links in, 38
  passwords in, 38
  protecting, 39–40, 40
  scripts in, 22
  spoofing, 37, 141
  embedded links, 36
enabling
  auditing, 105–110, 106, 108–109
  DSA events, 103
  firewalls, 16
Encapsulating Security Protocol (ESP), 165–166
Encrypt Message Contents And Attachments option, 228
Encrypting File System (EFS), 132, 231–234
encryption, 215
  AES, 217–219
  asymmetric, 219–222, 221
  BitLocker, 235–238, 235, 238
certificates, 222, 222, 243
  EFS, 231–234
  email, 226–228, 226–228
  exercises, 239
  hashing, 223–225, 223–224
  IPsec, 165–166, 165
  methods, 216
  offline folders, 132–133, 132–133
  review questions, 239–240
  summary, 238
  symmetric, 216–218, 217
  WEP, 175–176
Enforce Password History policy, 50–51
  enforcing strong passwords, 49–51, 49
Enhanced Security Configuration (ESC), 259–260,
  259–260
enterprise CAs, 254, 254
errors in certificates, 245–248, 246–248
ESC (Enhanced Security Configuration), 259–
  260, 259–260
ESP (Encapsulating Security Protocol), 165–166
event subscriptions, 103, 113, 113
Event Viewer, 100, 101, 113
Exchange Server, 29
explicit permission denies, 76
Extensible Authentication Protocol (EAP), 64, 178–179
Extensible Markup Language (XML) files, 13

F
failover clusters, 6
Failure events
   auditing, 97, 100
   enabling and disabling, 102
FAT filesystems
   auditing, 100
   with EFS, 234
   permissions, 81
fault-tolerant technologies, 6
Fax Server services, 138
Federal Information Processing Standards (FIPS), 177, 178
fences, 196
File Services role, 138
File Transfer Protocol (FTP), 150
files, copied, permissions with, 78–81, 80, 233–234
Filter Current Log page, 110–111, 111
filters
   InPrivate Filtering, 263–264, 264
   MAC, 187–188, 188
   packet, 148
   Security logs, 110–111, 111
   SmartScreen Filter, 272–273
fingerprints, 61
FIPS (Federal Information Processing Standards), 177, 178
firewalls, 153–154
   defense-in-depth strategy, 155
   enabling, 16
   honeypots, 159
   host-based and network-based, 154–155, 155
   for malware, 28
   NATs, 159
   UTMs and SCMs, 155–157
firmware-based keyloggers, 195
first-party cookies, 260
flood attacks, 148–149, 148
Floppy Drives setting, 210
folders, offline, 130–133, 132–133
Force Password Change permission, 90
Forefront Threat Management Gateway, 137, 156
freeware, 22
frequency in wireless security, 172
front-door access, 196
FTP (File Transfer Protocol), 150
Full Control permission, 71, 73, 75, 83, 89

G
General tab
   browser history, 265, 266
   certificates, 250, 250
   cookies, 262
   EFS, 231
   permissions, 73, 73
Generate Resultant Set of Policy (logging)
   permission, 90
Generate Resultant Set of Policy (planning)
   permission, 90
globally unique identifiers (GUIDs), 102
GPOs. See Group Policy objects (GPOs)
Group Policy, 194
   clients, 129–130, 130
   IPsec, 165, 165
   passwords, 49–51, 49
Group Policy Management console, 202
Group Policy Management Editor, 204–205, 205
Group Policy objects (GPOs), 200
   default, 200–201
   designing, 201–202, 201
   log on locally, 206–208, 207, 209
   Removable Storage Access policy, 209–211,
   210–211
   security settings, 204–206, 205
   users and computers management, 203–204, 204
IANA (Internet Assigned Numbers Authority), 152
IDEA (International Data Encryption Algorithm), 218
identification badges, 197
identification vs. authentication, 44–45
identifiers, virus, 31
identity, verifying, 35
IDSs (Intrusion Detection Systems), 147–148
IE. See Internet Explorer (IE) browser
IEEE 802.11 wireless standards
enforcement, 163
overview, 171–172
Windows 7 wireless settings, 181
IIS (Internet Information Services)
vulnerabilities, 115
impersonation, 34
implicit permission denies, 76
Important updates, 126–127
in-person social-engineering attacks, 34
Include Inheritable Permissions From This
Object's Parent option, 79
Infect Your PC rogueware, 24
inheritance
auditing, 107
permissions, 76–79, 77–79, 88, 92, 92
InPrivate Browsing, 263–265, 265
InPrivate Filtering, 263–264, 264
input validation for buffer-overflow attacks, 26
Install Updates Automatically (Recommended)
option, 128
installing MBSA, 116
integrity, 2
DNS records, 168
e-mail, 228–229
protecting, 6–7
interactive logons, 101
International Data Encryption Algorithm
(IDEA), 218
Internet Assigned Numbers Authority (IANA), 152

H

handprints, 61
hardening servers, 1, 10–11
antivirus software, 16
attack surfaces, 11–14, 11–14
firewalls, 16
system updates, 14–15
hardware-based keyloggers, 195
Hash software rule, 135
hashes, 6
defined, 165
e-mail, 229–231, 229–230
hashing algorithms, 223–225, 223–224
health certificates, 162–163
health policies, 161
Health Registration Authority (HRA), 162
Hellman, Martin, 222
heuristics component in antivirus software, 31
High alert level in Microsoft Security Essentials, 32
history, browser, 265, 266
hives, 91
honeypots, 159
Host (A) records, 140
host firewalls, 16, 154–155, 155
hosts file in pharming, 38–39
hotfixes, 14
HRA (Health Registration Authority), 162
HTTP (Hypertext Transfer Protocol), 11
HTTP with Secure Socket Layers (HTTPS), 11,
244–245, 244
hubs vs. switches, 199, 199–200
Hypertext Transfer Protocol (HTTP), 11
Internet Explorer (IE) browser, 257
add-ons, 266–268, 267
Advanced settings, 268–269, 268
browser history, 265, 266
cookies, 260–262, 261
Enhanced Security Configuration, 259–260, 259–260
exercises, 274
InPrivate Filtering and InPrivate Browsing, 263–265, 264–265
pop-up blockers, 262–263, 263
Protected Mode, 273
review questions, 274–275
security zones, 269–271, 270–271
settings, 257–259, 258
SmartScreen Filter, 272–273
summary, 273–274
“Internet Explorer has found a problem with this website’s security certificate” error, 247
Internet-facing servers, 157
Internet Information Services (IIS) vulnerabilities, 115
Internet Options dialog box
add-ons, 266–267, 267
Advanced tab, 268–269, 268
browser history, 265, 266
certificates, 248, 249
Privacy tab, 260–262, 261
security zones, 269–271, 270–271
Internet Protocol Security (IPsec) protocol enforcement, 163
mechanisms, 165–166, 165
for Telnet, 150
Internet zone, 269
intrusion-detection by SCM firewalls, 156
Intrusion Detection Systems (IDSs), 147–148
IP addresses
IPv6, 140
NAT, 159
wireless routers, 183
IP half-scan attacks, 149
ipconfig/displaydns command, 39
IPsec (Internet Protocol Security) protocol enforcement, 163
mechanisms, 165–166, 165
for Telnet, 150
iris scans, 61
isolating
networks, 159
servers, 157–158, 158
J
Junk E-mail folder, 40, 40
K
KDCs (Key Distribution Centers), 63
Kerberos
AES encryption, 177, 218
ports, 63
for time skew, 63–64
Key Distribution Centers (KDCs), 63
key fobs, 60
keyloggers, 27, 195
keys, 91
AES, 177, 219
asymmetric encryption, 219–222, 221
BitLocker Drive Encryption recovery, 236
certificates, 242–245, 244
EFS, 231–232
e-mail, 226–230, 226–227, 229–230
cipher, 175
PKI, 251
sharing, 222, 222
symmetric encryption, 216–217, 217
WEP, 176
keystroke loggers, 195
Kido worm, 22
Kismet sniffer, 186–187
L

L2TP (Layer 2 Tunneling Protocol), 167
LAN Manager (LM), 66
LAND (local area network denial) attacks, 151
Layer 2 Tunneling Protocol (L2TP), 167
least privilege principle, 9–10, 10, 35
limiting rights, 35
links, email, 36, 38
List Folder Contents permission, 71, 75
List Folder/Read Data permission, 72–73
LM (LAN Manager), 66
local area network denial (LAND) attacks, 151
Local Intranet zones, 269
local logons, 101
Local Security Policy tool
auditing, 96–97, 97, 105
logons, 206
password settings, 49–51
software restrictions, 133–134, I34
user rights, 104, I04
lockout policies, 51–53, 52
locks, cipher, 197–198
log on locally settings, 206–208, 207, 209
Log On tab, 10, I0
Logon policies, 98, 101–102
logs
audit, 96, 195
failed attempts, 97
Security, 100, 103
managing, 111–112
saving, 113, I13
securing, 113–114
viewing, 110–111, I10
Low alert level in Microsoft Security Essentials, 32

M

MAC (media access control) addresses, 187–188, I88
Mac OS X operating system vulnerabilities, 15
malicious ActiveX controls, 271
Malicious Software Removal Tool, 33, 33
malicious websites, 272–273
malware
administrator control by, 63
antivirus, 29–31, 29–30
and availability, 5
and botnets, 20–21
buffer-overflow attacks, 25–26, 25
exercises, 41
Microsoft Security Essentials for, 31–33, 32
mobile devices, 212
pop-ups, 263–264
principle of least privilege, 9–10
protecting against, 28–33
review questions, 41–42
spyware, 26–27
statistics on, 27–28
Stuxnet, 24–25
summary, 41
Trojan horses, 23–24, 24
types, 19–20
viruses, 21–22
worms, 22–23
man-made threats, 3
Manage Add-ons page, 266, 267
Manage BitLocker window, 236
Manage Wireless Networks settings, 181, I81, 189, I89
mantraps, 198
masked web addresses, 36, 36
matched pairs
asymmetric encryption, 221
certificates, 243
Maximum Password Age policy, 50
MBSA (Microsoft Baseline Security Analyzer), 95
installing, 116
running, 116–117
working with 114–116, I15
MD5 (Message Digest 5), 223, 223
media access control (MAC) addresses, 187–188, I88
Medium alert level in Microsoft Security Essentials, 32
member servers, 206
Message Digest 5 (MD5), 223, 223
MessageLabs Intelligence 2010 Annual Security Report, 27
Microsoft Baseline Security Analyzer (MBSA), 95
installing, 116
running, 116–117
working with 114–116, 115
Microsoft Challenge Handshake Authentication Protocol v2 (MS-CHAP v2), 65
Microsoft Point-to-Point Encryption (MPPE), 167
Microsoft Security Essentials
on desktops, 31–33, 32
scanning options, 30, 30
Microsoft TechNet download page, 224, 224
Microsoft Technology Associate Security Fundamentals certification, 3
Microsoft Update site, 126
Minimum Password Age policy, 50
Minimum Password Length policy, 50
mobile devices, 211–212
Modify permission, 71, 75
modifying data by attackers, 195
monitoring reboots, 104
Morris, Robert, 22
Morris worm, 22
motion detectors, 198
movable cameras, 196
moved files, permissions with, 79–81, 80, 233–234
moving objects into OUs, 203
MPPE (Microsoft Point-to-Point Encryption), 167
MS-CHAP v2 (Microsoft Challenge Handshake Authentication Protocol v2), 65
multifactor authentication, 44
“Myth vs. Reality: Wireless SSIDs” blog, 187

N
name resolution in pharming, 38–39
names for share permissions, 82
NAP. See Network Access Protection (NAP)
NT (network address translation), 159
in L2TP, 167
wireless routers, 174
National Institute of Standards and Technology (NIST), 2–3
Nessus tool, 47
Network Access Protection (NAP), 159
client health evaluation, 162–163, 162
components, 160–162, 161
enforcement methods, 163
overview, 159–160
requirements, 163–164
network address translation (NAT), 159
in L2TP, 167
wireless routers, 174
Network And Sharing Center, 181, 181, 189, 189
network interface cards (NICs), 158
Network Monitor, 150–151, 150
Network Policy role, 138
Network Zone software rule, 135
networks
attack methods, 147–148
auditing, 114–117, 115, 117
in defense-in-depth strategy, 8
denial of service attacks, 148–149, 148
distributed denial of service attacks, 149
exercises, 168
firewalls, 16, 153–159, 155, 158
NAP, 159–164, 161–162
protocol security methods, 164–168, 165, 167
review questions, 169
sniffing attacks, 149–151
spoofing attacks, 151
summary, 168
Never Check For Updates (Not Recommended) option, 128
Never Notify We When setting, 125
New Software Restriction Policies option, 133
New Technology Files System (NTFS)
permissions, 69, 81
vs. Active Directory permissions, 88
advanced, 71–75, 72–73
basic, 70–71, 70–71
share permissions combined with, 85–87
New Technology LAN Manager (NTLM) security protocol, 66
NICs (network interface cards), 158
NIST (National Institute of Standards and Technology), 2–3
No Authentication (Open) setting, 180
nonpromiscuous sniffer mode, 151
nonrepudiation, 96, 225, 230
Notify Me Only When Programs Try To Make Changes To My Computer (Do Not Dim My Desktop) option, 124–125
NSEC3 records, 168
NTFS. See New Technology Files System (NTFS) permissions
NTLM (New Technology LAN Manager) security protocol, 66
numbers in passwords, 48–49

O
object access auditing, 98–100, 100–101, 107, 108
objects, moving into OUs, 203
offline folders
  encrypting, 132–133, 132–133
  overview, 130–131
Offline Properties page, 132, 133
on-demand virus scans, 30–31
operating system updates, 14–15
Ophcrack tool, 46, 66
Optional updates, 126–127
organizational units (OUs), 200
  creating, 202–203
  designing, 201–202, 201
  moving objects into, 203
  permissions, 87–89
OS X operating system vulnerabilities, 15
out-of-band updates, 125
overflows, buffer
  description, 20
  overview, 25–26, 25
  updates for, 23
Overwrite Events As Needed (Oldest Events First) option, 112
Owner permission, 83

P
packet-filtering firewalls, 153
packet filters, 148
packet sniffers. See sniffers
Page menu in IE, 258
pairing mobile devices, 212
PAP (Password Authentication Protocol), 65
partitions in moving and copying files, 80, 80
Password Authentication Protocol (PAP), 65
Password Must Meet Complexity Requirements policy, 50
Password Policy, 49–51, 129, 206
password replication policies (PRPs), 139
password-reset disks, 58–59
Password Settings Object (PSO), 206

passwords
  Account Lockout Policy, 51–53, 52
  attacks on, 45–46
  BitLocker To Go, 237
  changing, 57–58
  in cookies, 262
  cracking, 46–47, 66
  in email, 38
  LAN Manager, 66
  MBSA for, 115
  overview, 45
  password-reset disks, 58–59
  resetting, 55–57, 55–56
  in social-engineering attacks, 35
  strong
    creating, 47–49
    enforcing, 49–51, 49
    unlocking accounts, 53–54, 53–54
  Windows 7 wireless settings, 180
  wireless routers, 183, 185
Patch Tuesday, 14
patches, 14, 26
Path software rule, 135
paths for shared resources, 81–82, 84
PEAP (Protected EAP) protocol, 64, 178–179
performance with SCM firewalls, 156
perimeter networks, 157–158, 158
permissions, 69
  Active Directory, 87–91, 88–90
  combining, 75–76, 76, 85–87
  exercises, 93
  inheritance, 76–79, 77–79, 88, 92, 92
  with moved and copied files, 78–81, 80, 233–234
NTFS. See New Technology Files System (NTFS) permissions
Registry, 91–92, 92
review questions, 93–94
Security logs, 114
share, 81–87, 84
summary, 93
Personal Identification Number (PINs), 44, 60, 236
personal information in email, 38
personally identifiable information (PII), 27
phishing
  protection from, 40
  recognizing, 35–38, 36
  SmartScreen Filter for, 272–273
  statistics on, 27
phone calls in social-engineering attacks, 34–35
physical addresses, 187
physical drives in moving and copying files, 80, 80
physical security, 7, 193
  access control, 196–198, 196
  in defense-in-depth strategy, 9
  exercises, 213
GPOs. See Group Policy objects (GPOs)
importance, 194–195
mobile devices, 211–212
review questions, 213–214
summary, 213
  switches, 199, 199–200
picture display, disabling, 40
piggybacking, 198
PII (personally identifiable information), 27
PINs (Personal Identification Number), 44, 60, 236
PKI. See Public Key Infrastructure (PKI)
Point-to-Point Tunneling Protocol (PPTP), 166–167
  poisoned DNS servers, 39
  policies in defense-in-depth strategy, 7–8
Policy Change policy, 99, 105
pop-unders, 263
pop-up blockers, 262–263, 263
port scans, 151–153
ports
  commonly used, 152–153
  Kerberos, 63
  wireless routers, 174
PPTP (Point-to-Point Tunneling Protocol), 166–167
  preshared keys (PSks), 177–178, 180
  principle of least privilege, 9–10, 10, 35
Print Services role, 138
privacy policies, 261–262, 261
private IP addresses, 159
private keys
  AES encryption, 177
  asymmetric encryption, 219–222, 221
  certificates, 242–245, 244
  EFS, 231–232
  email, 226–227, 226–227, 229, 229–230
  PKI, 251
Privilege Use policy, 99, 104–105, 104
procedures, 7–8
Process Tracking policy, 99, 105
promiscuous sniffer mode, 151
Protected EAP (PEAP) protocol, 64, 178–179
Protected Mode in IE, 273
Protected Mode indicator, 259
protocol security methods, 164
  DNSsec, 167–168
  IPsec, 165–166, 165
  tunneling, 166–167, 167
proximity cards, 197–198
proxy servers, 156
PRPs (password replication policies), 139
PSKs (preshared keys), 177–178, 180
PSO (Password Settings Object), 206
PTR (Pointer) records, 140
Public Key Infrastructure (PKI), 7, 241
certificate chains, 252–254, 252–253
certificate services, 254–255
components, 251–252
exercises, 255
review questions, 256
smart cards, 59–60
summary, 255
Public keys
AES encryption, 177
asymmetric encryption, 219–222, 221
certificates, 242–245, 244
EFS, 231
email, 226–227, 226–227, 229, 229–230
PKI, 251
sharing, 222, 222
Q
quarantined clients, 160
R
RADIUS (Remote Authentication Dial-in User Service), 64–65
RAIDs (Redundant Arrays of Independent Disks), 6
RAs (Registration Authorities), 252
Read & Execute permission, 70–71, 75
Read Attributes permission, 72–73
Read Extended Attributes permission, 72, 74
read-only domain controllers (RODCs), 139–140, 195
Read permission, 70–72, 75, 83, 89
Read Permissions permission, 74
Read/Write permission, 83
Reader permission, 83
real-time virus protection, 30
reboots, monitoring, 104
Recommended updates, 126–127
recovering passwords, 46
recovery agents, 233
recovery keys, 236
reducing attack surfaces, 11–14, 11–14
Redundant Arrays of Independent Disks (RAIDs), 6
regedit command, 91
Registration Authorities (RAs), 252
Registry Editor, 91–92, 92
Registry for permissions, 91–92, 92
regular UAC user tokens, 62
remote access
firewalls, 156
VPNs for, 157
Remote Authentication Dial-in User Service (RADIUS), 64–65
Remote Desktop Services, 138
Removable Disks setting, 210
Removable Storage Access policy, 209–211, 210–211
removing inherited permissions, 78
Replace All Existing Inheritable Permissions On All Descendants With Inheritable Permissions From This Object option, 92
Reply To address, 37
Reset Account Lockout Counter After setting, 52
Reset User Passwords And Force Password Change At Next Logon option, 90
resetting passwords
in social-engineering attacks, 35, 57
steps in, 55–57, 55–56
restricted networks, 162
restricted sites zone, 270
retina scans, 61
reverse-engineering updates, 126
revocation dates in CRLs, 246
rights, limiting, 35
Riley, Steve, 187
Risk overview, 1–4, 2
Rivest, Ronald, 222
RODCs (read-only domain controllers), 139–140, 195
rogueware, 23–24, 24
roles
    share, 83
        Windows Server, 137–138, 137
root CAs, 252, 255
routers, wireless, 173–174, 174, 183
default passwords, 183, 185
MAC filtering, 187–188, 188
SSIDs
    broadcasting, 185–187, 187
    changing, 183–185
routing SCM firewalls, 156
RSA algorithm, 222
rules in software-restriction policies, 133–135, 134
Run As Administrator command, 61–62, 62
Rustock botnet, 27

S
S/MIME (Secure/Multipurpose Internet Mail Extensions), 225
SACLs (system access control lists), 99–100
Safety menu in IE, 258
SAM (Security Account Manager) databases, 44, 101
sandboxes, 31
Sasser worm, 23
saving logs, 113, 113
scans
    antivirus software, 30–31
    port, 151–153
SCCM (System Center Configuration Manager), 15, 128–129, 129
scheduled antivirus scans, 30
SCM (secure content management) firewalls, 155–157
scripts, viruses in, 22
SCW (Security Configuration Wizard), 12–14, 12–14
secret keys
    asymmetric encryption, 220–221, 221
certificates, 245
EFS, 231
    email encryption, 226–227, 226–227
    symmetric encryption, 216
secure content management (SCM) firewalls, 155–157
secure Desktop, 123
secure dynamic updates, 142–143, 143
Secure Hashing Algorithm (SHA), 223, 223
Secure/Multipurpose Internet Mail Extensions (S/MIME), 225
Secure Server (Require Security) policy, 166
Secure Socket Layer (SSL), 167
Secure Socket Tunneling Protocol (SSTP), 167
Security Account Manager (SAM) databases, 44, 101
Security Configuration Wizard (SCW), 12–14, 12–14
security guards, 197
Security logs, 100, 103
    managing, 111–112
    saving, 113, 113
    securing, 113–114
    viewing, 110–111, 110
Security Policy File Name page, 12–13, 13
Security tab
    permissions, 89, 89
    Windows 7 wireless settings, 181–182, 182
security triad, 1, 4–5, 4
    availability, 5–6
    confidentiality, 5
    integrity, 6–7
security zones in IE, 269–271, 270–271
Sender Policy Framework (SPF) records, 140–141
separate VLANs, 136–138, 136–137
serial numbers for CRLs, 246
Server (Request Security) policy, 166
server room access, 198
servers, 135
    in defense-in-depth strategy, 8
    DNS security issues, 140–143, 142–143
    exercises, 144
    hardening. See hardening servers
    isolating, 157–158, 158
service accounts • Start This Connection Automatically option

member, 206
review questions, 144–145
RODCs, 139–140
summary, 144
UAC, 62, 123–125, 124
updating, 125–130, 127, 129–130
VLANs for, 136–138, 136–137

service accounts, 10
Service (SRV) records, 140
session keys, 245
Severe alert level in Microsoft Security Essentials, 32
SHA (Secure Hashing Algorithm), 223, 223
Shamir, Adi, 222
share permissions, 81–82
  combining, 85–87
  identifying, 83–85, 84
Share Roles permission, 83
Shared Folder Permissions page, 82, 82
Shared setting for wireless security, 180
shares, creating, 84, 84
shareware, 22
sharing public keys, 222, 222
SHAs (System Health Agent), 160–161
SHVs (System Health Validators), 161, 161
signatures, 225, 228–231, 229–230, 243
signed ActiveX controls, 270–271
silent alarms, 198
Simple Mail Transport Protocol (SMTP), 11
site security, 194
size of Security logs, 112, 112
smart cards
  authentication, 59–60, 59–60
  with RADIUS, 65
SmartScreen Filter, 272–273
SMTP (Simple Mail Transport Protocol), 11
sniffers
  attacks using, 149–151
  description, 34, 165
  with hubs, 199, 199
  with switches, 199, 200
wireless, 186–187
Snow Leopard system, 15

social-engineering attacks
  exercises, 41
  overview, 34
  passwords, 45–46, 57
  in person, 34
  pharming, 38–39
  phishing, 35–38, 36
  with phone calls, 34–35
  review questions, 41–42
  summary, 41
software-based keyloggers, 195
software-restriction policies, 133–135, 134
something you are, 44
something you have, 44
something you know, 44
spam
  antispam techniques, 39–40
  dealing with, 29
  defined, 21
  statistics on, 27
spammers, spoofing by, 141
spear phishing, 37
speed of wireless security, 172
SPF (Sender Policy Framework) records, 140–141
spoofing attacks
  description, 151
  email, 37, 141
  MAC addresses, 188
spyware
  description, 20
  overview, 26–27
SQL administrative vulnerabilities, 116
SRV (Service) records, 140
SSH for Telnet, 150
SSIDs
  broadcasting, 185–187, 187
  changing, 183–185
SSL (Secure Socket Layer), 167
SSTP (Secure Socket Tunneling Protocol), 167
standalone CAs, 254–255
standards for wireless security, 171–172
Start This Connection Automatically option, 190
starting applications with Run As Administrator, 61–62, 62
stateful-filtering firewalls, 153
stealing
data, 195
systems, 194–195
Store Passwords Using Reversible Encryption policy, 50
stream ciphers, 175–176
strong passwords
creating, 47–49
enforcing, 49–51, 49
Stuxnet malware, 24–25
subscriptions, event, 103
Success events
auditing, 97, 100
enabling and disabling, 102
supplicants in WPA2, 178
switches vs. hubs, 199, 199–200
symbols in passwords, 48–49
symmetric encryption, 175
AES, 177
vs. asymmetric, 220
e-mail, 226–228
overview, 216–218, 217
SYN flood attacks, 148–149, 148
synchronize (SYN) flag, 148–149, 148
system access control lists (SACLs), 99–100
System Center Configuration Manager (SCCM), 15, 128–129, 129
system events, 103
System Events policy, 98
System Health Agent (SHAs), 160–161
System Health Validators (SHVs), 161, 161
System Statement of Health, 161
systems, updating, 14–15

T
tailgating, 198
Take Ownership permission, 73–74

Tape Drives setting, 210
telnet service, 11, 150
Temporal Key Integrity Protocol (TKIP), 176
Terminal Services, 138
testing for buffer-overflow attacks, 26
theft
data, 195
systems, 194–195
“There is a problem with this website’s security certificate” error, 247, 248
third-party cookies, 260–261
“This website’s security certificate has been revoked” error, 247
“This website’s security certificate is out of date” error, 247
“This website’s security certificate isn’t from a trusted source” error, 247
Threat Management Gateway (TMG), 137, 156
three-pronged firewall configuration, 158
time skew, Kerberos for, 63–64
TKIP (Temporal Key Integrity Protocol), 176
TMG (Threat Management Gateway), 137, 156
tokens and token devices
administrative accounts, 122
authentication, 59–60, 59–60
UAC, 62
Tools menu in IE, 258
TPM (Trusted Platform Module), 236
Traverse Folder/Execute File permission, 73
triad, security, 1, 4–5, 4
availability, 5–6
confidentiality, 5
integrity, 6–7
Triple DES (3DES) encryption, 218
Trojan horses
and availability, 5
description, 20
overview, 23–24, 24
Trusted Platform Module (TPM), 236
Trusted Root Certification Authorities store, 248–249, 249, 252–255
trusted sites zone, 270

tunneling protocols, 166–167, 167

turnstiles, 198

twofish algorithm, 218

U

UAC (User Account Control), 62, 122–123, 122–123
dimmed Desktop, 123
settings, 123–125, 124
UDDI (Universal Description, Discovery, and Integration) services, 138
unauthorized software, 194
unexpected data in buffer-overflow attacks, 26
unified threat management (UTM) firewalls, 155–157
Universal Description, Discovery, and Integration (UDDI) services, 138
Universal Naming Convention (UNC) paths, 81–82, 84
Unlock Account option, 54
Unlock The User’s Account option, 55
unlocking accounts, 53–54, 53–54
Unrestricted software rule, 134, 134
unsafe downloads, 273
unscheduled reboots, 104
unsecure authentication protocols, 65–66
updates
Automatic Updates, 126–128, 127
for buffer-overflow attacks, 26
DNS, 141–143, 142–143
importance, 125–126
for malware, 28
MBSA for, 116
reverse-engineering, 126
systems, 14–15
with WSUS and SCCM, 128–129, 129–130
URLs, masked, 36, 36
USB drives
BitLocker, 235–237
password-reset disks, 58–59
stealing, 195
Stuxnet malware, 24
viruses on, 22
USB wireless adapters, 172
Use A Password To Unlock The Drive option, 237
User Account Control (UAC), 62, 122–123, 122–123
dimmed Desktop, 123
settings, 123–125, 124
User Account Control dialog box, 122–123, 122–123
User Account Control Settings dialog box, 124, 124
User Configuration node, 204
User Must Change Password At Next Logon option, 55, 90
User Rights Assignment node, 104, 104, 206, 207
usernames
in cookies, 262
in social-engineering attacks, 35
users and user accounts
auditing, 103
authenticating. See authentication
educating, 28
GPOs for, 203–204, 204
UTM (unified threat management) firewalls, 155–157

V

validating certificates, 246–247, 247
vendors for updates, 125
verifying identity, 35
version 1 certificates, 246
version 2 certificates, 246
version 3 certificates, 246
viewing
Active Directory permissions, 88–91, 89–90
audit information, 110–111, 110–111
MBSA reports, 117, 117
virtual local area networks (VLANS), 136–138, 136–137
virtual machines, 31
virtual private networks (VPNs)
  enforcement, 162–163, 162
  in NAP, 164
  RADIUS for, 64
  for remote access, 156–157
viruses
  and availability, 5
  description, 20
  in email scripts, 22
  overview, 21–22
  protection from. See antivirus (AV) software and techniques
VLANs (virtual local area networks), 136–138, 136–137
VPNs. See virtual private networks (VPNs)
Vulnerabilities
  exploitation of, 2
  as weaknesses, 3
  zero-day, 125

W
walls for perimeter networks, 157–158, 158
WAPs (wireless access points), 149–150, 173, 173
  war driving, 184, 184
WDS (Windows Deployment Services), 138
  web addresses, masked, 36, 36
  web browsers. See Internet Explorer (IE) browser
  Web Server (IIS) services, 138
  weight in authentication, 61
  well-known ports, 151–153
  WEP (Wired Equivalent Privacy) protocol, 174–176
  Wi-Fi Protected Access (WPA), 176
  Wi-Fi Protected Access version 2 (WPA2), 177–178, 178–179
  Windows 7 wireless settings, 179–182, 180–182, 189–190, 189
  Windows Deployment Services (WDS), 138
  Windows Explorer for shares, 84, 84
  Windows Firewall, 16
Windows Server Update Services (WSUS), 15, 128–129, 129–130
Windows Update, 126
Wired Equivalent Privacy (WEP) protocol, 174–176
wireless access points (WAPs), 149–150, 173, 173
wireless networks in defense-in-depth strategy, 9
wireless routers, 173–174, 174, 183
  default passwords, 183, 185
  MAC filtering, 187–188, 188
  SSIDs
    broadcasting, 185–187, 187
    changing, 183–185
wireless security, 171
  adapters, 172
  encryption keys, 175
  exercises, 190
  Extensible Authentication Protocol, 178–179
  review questions, 191
  routers. See wireless routers
  standards, 171–172
  summary, 190
  WAPs, 173, 173
  WEP, 175–176
  Wi-Fi Protected Access version 2, 177–178, 178–179
  Windows 7 settings, 179–182, 180–182, 189–190, 189
  WPA, 176
wireless sniffers, 34
WORM (Write Once Read Many) DVDs, 114
worms
  and availability, 5
  description, 20
  overview, 22–23
  WPA (Wi-Fi Protected Access), 176
  WPA-Enterprise, 178, 181
  WPA-Personal, 177, 180
  WPA2 (Wi-Fi Protected Access version 2), 177–178, 178–179
  WPA2-Enterprise, 178, 181
  WPA2-Personal, 177, 180
WPD Devices setting, 210
Write attributes permission, 74
Write Extended Attributes permission, 74
Write Once Read Many (WORM) DVDs, 114
Write permission, 71, 75, 89
WSUS (Windows Server Update Services), 15, 128–129, 129–130

X

XML (Extensible Markup Language) files, 13

Z

zero-day attacks, 125
zero-day vulnerabilities, 125
zombies in DoS attacks, 149
Zone indicator, 259
zones
  DNS, 143
  security, 269–271, 270–271